Maastricht University

Datenschutz in Europa

Citation for published version (APA):

Lavranos, N. (1996). Datenschutz in Europa: Am Beispiel der Datenschutzrichtlinie, des Schengen Information Systems (SIS) und Europol. *Datenschutz und Datensicherheit*, *1996*(July), 400-406.

Document status and date:
Published: 01/01/1996

Document Version:
Accepted author manuscript (Peer reviewed / editorial board version)

Please check the document version of this publication:

• A submitted manuscript is the version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher's website.
• The final author version and the galley proof are versions of the publication after peer review.
• The final published version features the final layout of the paper including the volume, issue and page numbers.

Link to publication

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

• Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
• You may not further distribute the material or use it for any profit-making activity or commercial gain
• You may freely distribute the URL identifying the publication in the public portal.

If the publication is distributed under the terms of Article 25fa of the Dutch Copyright Act, indicated by the “Taverne” license above, please follow below link for the End User Agreement:

www.umlib.nl/taverne-license

Take down policy
If you believe that this document breaches copyright please contact us at:

repository@maastrichtuniversity.nl

providing details and we will investigate your claim.

Download date: 05 May. 2023

In: DuD 1996, pp.400-406.

Datenschutz in Europa

Am Beispiel der Datenschutzrichtlinie, des Schengen Information Systems (SIS) und Europol

Einleitung und Problemstellung

Mit der vorliegenden Arbeit soll das Thema Datenschutz in Europa mit seinen vielschichtigen Problemen zunächst rechtlich eingeordnet werden, um in einem zweiten Schritt kritisch den derzeitigen Stand und die mögli-che zukünftige Entwicklung des Datenschutz auf europäischer Ebene zu beleuchten.

Zunächst stellt sich die Frage, welchen Stellenwert der Datenschutz auf internationaler und supranationaler Ebene hat und mit welchen Interessen der Datenschutz kollidiert.

Datenschutz ist eine relativ junge Erscheinung, die sehr eng mit der Ent-wicklung des Computers zusammenhängt. Erst seit der Computer Mitte der 70er Jahre auf immer neuen Gebieten eingesetzt wird, tritt der Daten-schutz zunehmend in den Vordergrund.

Am Anfang war Datenschutz eine rein nationale Angelegenheit; nach und nach verabschiedeten einige europäische Staaten die ersten Datenschutz-gesetze, wobei Hessen im Jahre 1970 mit dem Hessischen Datenschutzge-setz (HDSG) eine weltweite Vorreiterrolle spielte.

Doch sehr schnell wurde deutlich, daß aufgrund der zunehmenden inter-nationalen wirtschaftlichen Verflechtung die Vernetzung von Datenban-ken auf nationaler wie internationaler Ebene forciert wurde. Damit nahm der grenzüberschreitende Datenverkehr kontinuierlich zu, so daß der grenzüberschreitenden Datenschutz zu einer der zentralen Fragen wurde.[1]

Daraufhin verabschiedete der Rat der Organisation für Wirtschaftliche Zusammenarbeit und Entwicklung (OECD) im September 1980 Leitlinien für den Schutz der Privatsphäre bei grenzüberschreitenden Datenverkehr. Parallel zu den Bemühungen in der OECD, beschloß im Jahre 1981 der Europarat die Konvention zum Schutz des Einzelnen im Hinblick auf die automatische Verarbeitung personenbezogener Daten (EuDSK), die am 1. Oktober 1985 als „erste völkerrechtlich verbindliche Datenschutzrege-lung“ in Kraft trat.[2]

Aber auch im Rahmen der Europäischen Gemeinschaft (EG) wurde das Thema Datenschutz diskutiert. Zunächst nur sehr zögerlich und dann auch nur vom Europäischen Parlament. Das Europäische Parlament forderte mehrmals die Europäische Kommission auf, endlich auf dem Gebiet des Datenschutzes tätig zu werden - zunächst ohne Erfolg.[3]

Dies änderte sich jedoch infolge der Europäischen Einheits Akte (EEA) von 1987 in der im jetzigen Art. 7a EGV der freie Binnenmarkt innerhalb der EG bis zum 31.12.1992 beschlossen wurde. Das bedeutet, daß auch der Binnenmarkt des Datenverkehrs ebenfalls ohne Hindernisse funktio-nieren soll.

Der Vertrag über die Europäische Union (EUV) von Maastricht 1992 fügte eine weitere datenschutzrechtlich relevante Ebene hinzu. Durch Titel VI, Art. K ff. des EUV wurde eine engere Kooperation im Bereich der Inneren Sicherheit und Justiz und damit einhergehend ein intensiver Da-tenaustausch in der grenzüberschreitenden Polizeiarbeit vereinbart. Hier-durch wurde ein neuer sensibler Bereich erfaßt. Insbesondere in Gestalt des Europäischen Polizeiamtes (Europol) Art. K 1, Nr.

9 EUV und das durch das Schengener Abkommen eingerichtete Schengen Information System (SIS) erreicht die Kooperation auf europäischer Ebene im polizei-lichen Bereich eine neue ungekannte Qualität.[4]

Aber auch die Entwicklung des Datenschutzes auf nationaler Ebene, ins-besondere in Deutschland, hat Auswirkungen auf die Entwicklung des europäischen Datenschutzes. An erster Stelle ist hier das Volkszählungs-urteil des BVerfG[5] zu nennen, welches das Recht auf informationelle Selbstbestimmung (RiS) zu einem Grundrecht, abgeleitet aus Art. 2 I iVm Art. 1 I GG, erhoben hat. Problematisch ist hier, daß der EGV immer noch keinen eigenen Grundrechtskatalog enthält.[6] In diesem Zusammen-hang ist auch auf das Maastricht-Urteil des BVerfG[7] hinzuweisen, daß einen Grundrechtsschutz auf EG-Ebene verlangt, der dem deutschen Grundrechtsschutz entspricht.[8] Einen solchen Grundrechtsschutz könnte die Europäische Menschenrechts Konvention (EMRK) bieten, auf die auch der Europäische Gerichtshof (EuGH) zurückgreift[9], in der nach ganz überwiegender Meinung ein Recht auf informationelle Selbstbestimmung durch Art. 8 I EMRK verbürgt wird.[10]

Der Gang der Untersuchung gliedert sich wie folgt. Zunächst ist kurz auf die OECD-Leitlinien und die EuDSK einzugehen. Daraufhin wird die am 24. Oktober 1995 vom Europäischen Parlament und dem Rat der Europäischen Union verabschiedete Daten-schutzrichtlinie 95/46/EG[11] in einigen wichtigen Punkten analysiert und insbesondere mit dem Bundesdatenschutzgesetz (BDSG) verglichen.

Anschließend soll speziell auf die datenschutzrechtliche Situation beim SIS und bei Europol eingegangen werden. Abschließend folgt ein zusam-menfassendes Ergebnis und ein Ausblick auf die zukünftige Entwicklung des europäischen Datenschutzes.

I. Datenschutzrecht im Rahmen der OECD und des Europarats

Neben den Bemühungen auf der Ebene der Vereinten Nationen und ihren Sonderorganisationen um einen Mindeststandard an Datenschutz, auf die hier nicht weiter eingegangen werden kann[12], sind die OECD und der Europarat die Foren, in denen der grenzüberschreitenden Datenschutz behandelt wird.[13]

1. Datenschutzleitlinien der OECD

Zunächst ist anzumerken, daß die OECD-Leitlinien nur Teil einer unver-bindlichen Empfehlung an die Mitgliedstaaten sind und somit nicht in nationales Recht umgesetzt werden müssen.[14] Dies ist der entscheidende Schwachpunkt dieser Leitlinien, da sie in ihrer Wirkung äußerst begrenzt geblieben sind. Die OECD-Leitlinien orientieren sich an den Wachstums- und Wohlstandszielen der OECD-Konvention. Daher verwundert es nicht, daß es hauptsächlich darum geht, die nationalen Differenzen im Daten-schutz der Mitgliedstaaten zu minimieren, um mögliche Beschränkungen des grenzüberschreitenden Datenverkehrs zu beseitigen. Es geht somit vorrangig darum, dem grenzüberschreitenden Datenverkehr mögliche technische oder rechtliche Hindernisse innerhalb der OECD aus dem Weg zu räumen und weniger um die Schaffung eines effektiven grenzüber-schreitenden Datenschutzes. Immerhin enthalten die OECD-Leitlinien grundlegende Prinzipien wie etwa das Prinzip der Erhebungsbeschrän-kung, der Zweckbestimmung und der Verwendungsbeschränkung.[15]

Diese Prinzipien stellen den Grundkonsens der Mitgliedstaaten dar. Mithin kann man die OECD-Leitlinien zumindest als Spiegelbild des politischen Willens der OECD-Staaten nehmen.

2. Datenschutzkonvention des Europarats

Die Datenschutzkonvention des Europarats (EuDSK) geht gegenüber den OECD-Leitlinien schon weiter. Die EuDSK enthält die Verpflichtung, die Bestimmungen in nationales Recht umzusetzen (Art.

4 I EuDSK), jedoch können keine unmittelbaren Rechte aus der Konvention abgeleitet werden. Es handelt sich hierbei um ein „non-self-executing“ Dokument.[16] Weiterhin verweist Art. 12 EuDSK auf die Art. 10 EMRK (Recht auf Informationsfreiheit) und Art. 8 I EMRK (Schutz der Privatsphäre des Einzelnen).

An diesem Punkt wird das Spannungsfeld zwischen ungehinderten grenz-überschreitenden Datenverkehr und dem Erfordernis eines grenzüber-schreitenden Datenschutzes deutlich. Hier zeigt sich, die wichtige Funk-tion, welche die EMRK auch im Bereich des Datenschutzes auf euro-päischer Ebene hat.

Jedoch, insbesondere wegen Art. 12 II EuDSK, der das grundsätzliche Verbot enthält, Informa-tionsübermittlungen allein aus Gründen des Datenschutzes zu untersagen, bleibt das Schutzniveau der EuDSK niedrig. Art. 12 II ist daher der größte Schwachpunkt der Konvention, da es das Schutzniveau auf das niedrigste innerhalb der Unterzeichner- staaten der EuDSK herun-terdrückt.[17]

II. Die Datenschutzrichtlinie

1. Geschichte der Datenschutzrichtlinie

Die Datenschutzrichtlinie blickt auf eine lange Geschichte zurück, die bis in die 70er Jahre zurückreicht. Nach mehrmaligen Resolutionen des Euro-päischen Parlaments und Aufforderungen an die Europäische Kommission endlich auf dem Gebiet des Datenschutzes tätig zu werden, war der Beschluß der EuDSK im Jahre 1981 erstmalig Anlaß für die Europäische Kommission gewesen, die EG-Mitgliedstaaten aufzufordern die EuDSK zu ratifizieren.[18] Mit dieser Empfehlung glaubte die Europäische Kom-mission das Problem des Datenschutzes in der EG gelöst zu haben.

Doch schon 1982 forderte abermals das Europäische Parlament die Euro-päische Kommission auf eine Datenschutzrichtlinie vorzulegen. Erst 1990 legte die Europäische Kommission einen ersten Entwurf einer Daten-schutzrichtlinie[19] vor. Nach heftiger Kritik aus den Mitgliedstaaten, der Entwurf sehe ein zu hohes Schutzniveau vor und aus dem Europäischen Parlament, daß der Entwurf keinen ausreichenden Datenschutz gewähr-leiste, gab das Europäische Parlament im März 1992 seine Stellungnahme zu dem Entwurf ab. Dabei forderte das Parlament teilweise drastische Verschärfungen.[20] Am 15. Oktober 1992 legte die Europäische Kommission den zweiten Entwurf[21] vor, in dem die Änderungsvorschläge des Parlaments größtenteils berücksichtigt wurden. Der Zeitplan sah vor, daß die Datenschutzrichtlinie bis zum 1. Juli 1994 in nationales Recht umzusetzen ist. Davon war man jedoch weit entfernt. Erst am 24. Oktober 1995 verabschiedete der Rat der Europäischen Union die Datenschutz-richtlinie, wobei den Mitgliedstaaten eine Frist von drei Jahren bis zur Umsetzung der Datenschutzrichtlinie eingeräumt wird (Art. 32 I).

Die Tatsache, daß es mehr als 5 Jahre gedauert hat bis die Richtlinie beschlossen wurde, ist als Zeichen für das geringe Interesse der Mit-gliedstaaten gewertet werden, einen wirksamen Datenschutz auf europäi-scher Ebene zu schaffen.

2. Die Datenschutzrichtlinie

Bereits aus dem Titel „Richtlinie zum Schutz natürlicher Perso-nen bei der Verarbeitung personenbezogener Daten und zum Schutz des freien Datenverkehrs“ wird das Dilemma zwischen Datenschutz auf der einen Seite und funktionsfähigem Binnenmarkt bezüglich dem Datenver-kehr auf der anderen Seite deutlich.

Als Rechtsgrundlage für die Datenschutzrichtlinie wählte die Europäische Kommission Art. 100a EGV, da für die Errichtung und das Funktionieren des Binnenmarktes gem. Art. 7a EGV es erforderlich sei, daß personen-bezogene Daten von einem Mitgliedstaat in einen anderen Mitgliedstaat übermittelt werden können[22].

Der Gegenstand der Datenschutzrichtlinie ist in Art. 1 I genannt, wonach der Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten gewährleistet werden soll.

Die Datenschutzrichtlinie bezieht sich grundsätzlich auf alle personenbe-zogenen Daten, welche verarbeitet werden. Dabei umfaßt die Richtlinie die automatisierte sowie die nicht-automatisierte Verarbeitung von Daten, die in Dateien gespeichert sind oder gespeichert werden (Art. 3 I). Ent-scheidend ist somit, ob die Daten in Dateien geführt werden. Hierbei wer-den Akten grundsätzlich nicht von der Richtlinie erfaßt.[23] Dies entspricht dem § 1 II BDSG.

Der Begriff der Verarbeitung umfaßt explizit die Datenerhebung, sowie die Organisation, Ausarbeitung, das Abfragen, neben der Verarbeitung jede andere Form der Bereitstellung, die Kombination und das Vernichten von Daten (Art. 2 b).[24] Dies entspricht dem Begriff des Verarbeitens im Sinne von § 3 IV, V, VI BDSG.

Von ganz entscheidender Bedeutung ist die, nach dem Änderungsvor-schlag des Europäischen Parlaments, aufgehobene Trennung zwischen der Datenverarbeitung im öffentlich-rechtlichen und privatrechtlichen Bereich. Dies erweitert den Anwendungsbereich des Richtlinienentwurfs ganz erheblich und trägt zudem der Entwicklung Rechnung, daß zunehmend auch im privatrechtlichen Bereich, insbesondere bei multinationalen Unternehmen, personenbezogene Daten auch grenzüberschreitend gespeichert und ver-arbeitet werden.

Es geht somit beim Datenschutz nicht mehr vorrangig um ein Abwehr-recht gegenüber dem Staat, denn der Staat braucht nicht mehr selbst die Daten zu sammeln,[25] sondern braucht nur noch bei privaten Datensammlern „zuzugreifen“.[26] Dies ist wohl die entscheidende Richtungsänderung in der Informationstechnologie und damit auch im Datenschutz.

Dagegen herrscht im BDSG, ebenso wie bei den Landesdatenschutzge-setzen, die nicht mehr zeitgemäße strikte Trennung zwischen dem öffent-lich-rechtlichen und privatrechtlichen Bereich, wonach das BDSG nur im öffentli-ch-rechtlichen Bereich Anwendung findet.[27]

Ein weiterer wichtiger Punkt ist die Zweckbindung. Hier geht die Daten-schutzrichtlinie über das BDSG und der EuDSK hinaus. Danach muß die Zweckbindung schon bei der Datenerhebung und nicht erst bei der Spei-cherung vorliegen. Weiterhin muß das Ziel der Verarbeitung möglichst präzise bestimmt sein. Eine Zweckänderung ist nur dann erlaubt, wenn sie mit der ursprünglichen Zweckbestimmung vereinbar ist.

Hinsichtlich der Verarbeitung personenbezogener Daten aus „allgemein zugänglichen Quellen“ sieht die Richtlinie im Gegensatz zum ersten Ent-wurf ein Verbot der Verarbeitung solcher Daten vor, da nach Meinung der Europäischen Kommission, auch bei „allgemein zugänglichen Quel-len“, wie etwa Telefonbüchern, durchaus sensible personenbezogene Daten enthalten sein können. Dies geht ebenfalls über die Regelung der §§ 28 I, Nr. 3, 29 I, Nr. 2 BDSG hinaus.

Schließlich enthält die Richtlinie Befugnisse für die staatliche Daten-schutzkontrolle. Die Kontrollbehörden haben die Aufgabe, den Schutz personenbezogener Daten zu gewährleisten und müssen unabhängig sein. Dafür sieht die Richtlinie eine ganze Reihe von Interventionsbefugnissen vor, wie z.B. die Anordnung der Löschung von Daten, vorläufiges oder endgültiges Verbot der Verarbeitung, Vernichtung des Datenträgers und Verwarnung an den Verarbeiter (Art. 28). Diese Befugnisse gehen weit über denen, welche in § 38 V BDSG vorgesehen sind. Weiterhin haben die Kontrollbehörde die Pflicht zur Zusammenarbeit mit anderen Kon-trollbehörden sowie die Veröffentlichung von jährlichen Tätigkeitsberich-ten (Art. 30).

3. Bewertung der Datenschutzrichtlinie

Die kurze Darstellung einiger wichtiger Punkte der Datenschutzrichtlinie hat gezeigt, daß diese teilweise ein höheres Schutzniveau als das BDSG aufweist.[28]

Dennoch muß gefragt werden, ob die Datenschutzrichtlinie wirklich einen effektiven Datenschutz auf hohem Niveau garantieren kann.

Um dies beurteilen zu können, muß auf die Beweggründe und die Interes-sen, welche bei der Gestaltung der Richtlinien mitgewirkt haben einge-gangen werden.

Als erstes stellt sich die Frage, wieso bei der Ergänzung des EWGV durch die EEA im Jahre 1987 der Datenschutz mit keinem Wort erwähnt wurde. Hierfür hätten sich die eingefügten Art. 130f - 130q EGV bestens geeig-net, insbesondere da zu diesem Zeitpunkt das Volkszählungsurteil und die EuDSK sich bereits rechtlich etabliert hatten.[29]

Die Antwort liegt auf der Hand. Die bisherigen Aktivitäten der EG sind einseitig auf die wirtschaftlichen Gesichtspunkte orientiert, wobei der Datenschutz eher als Hindernis auf dem Weg zu einem freien Binnenmarkt des Datenverkehrs gesehen wird.[30]

Dies drückt sich vor allen Dingen in Art. 1 II der Datenschutzrichtlinie aus, wonach die Mitgliedstaaten den freien Verkehr von personenbezoge-nen Daten aus Datenschutzgründen nicht beschränken oder untersagen dürfen. Danach dürfen die Divergenzen bezüglich des Datenschutzniveaus nicht herangezogen werden, „um die freie Übermittlung von personenbe-zogenen Daten zwischen Mitgliedstaaten zu verbieten“. Das entspricht der Regelung des Art. 12 II EuDSK.[31] Weiterhin sollen die Mitgliedstaaten daran gehindert werden, ihre eigenen nationalen Datenschutzgesetze anzuwenden, wenn sie strenger sind als jene der anderen Mitgliedstaaten. Dies führt zu erheblichen verfassungsrechtlichen Probleme, wenn die An-wendung der Datenschutz- gesetze aus verfassungsrechtlichen Anforderun-gen abgeleitet ist,[32] was gerade für die Bundesrepublik Deutschland zu trifft, wie das Volkszählungsurteil des BVerfG[33] belegt. Im Lichte des Maastricht-Urteils[34] erscheint es zweifelhaft, ob eine solche Regelung mit dem vom BVerfG vorgegebenen Anforderungen an dem in der Europäischen Gemeinschaft zu gewährleistenden Grundrechtsschutz vereinbar ist.[35] Jedenfalls ist zu befürchten, daß aufgrund dieser Regelung das Datenschutzniveau auf das Niveau des Mitgliedstaats absinkt, welches das niedriges Datenschutzniveau aufweist.

Insofern ist die Befürchtung von Riegel, daß aufgrund des Vorrangs des Gemeinschaftsrechts gegenüber dem nationalen Recht, strengere Daten-schutz- vorschriften „niedergewalzt“ werden könnten, wenn sie sich gegen die Grundfreiheiten des freien Marktes wenden, nicht unbegründet.[36]

In diesem Zusammenhang ist auch das Problem der „Datenoasen“ zu sehen. Hoher Datenschutz bedeutet erhöhten technischen und personellen Aufwand, der wiederum die Kosten erhöht. Logische Folge davon ist, daß die Unternehmen bestrebt sein werden, ihre Datenverarbeitung in ein Land zu verlagern, welches kein oder nur ein geringes Datenschutzniveau auf-weist.[37] Folglich bringt geringer oder kein Datenschutz Wettbewerbsvorteile.[38] Es leuchtet ein, daß die Europäische Kommission vermeiden möchte, daß Unternehmen ihre Datenverarbeitung nach außer-halb der EG verlegen. Dies muß konsequenter Weise dazu führen, daß ein hohes Datenschutzniveau innerhalb der EG, welches spürbar höher ist als das der Nicht-EG-Staaten, nicht erwünscht sein kann.

Die Europäische Kommission hat dieses Problem erkannt und in der Richtlinie eine Regelung eingefügt, wonach die Datenweitergabe in Dritt-länder nur bei Vorhandensein eines „angemessenen“ Schutzniveaus er-laubt sein soll (Art. 25 I). Fraglich bleibt allerdings, was unter einem „angemessen“ Schutzniveau zu verstehen ist und welcher Maßstab hierfür zu nehmen ist. In Art. 25 II heißt es „die Angemessenheit des Schutzni-veaus, das ein Drittland bietet, wird unter Berücksichtigung aller Um-stände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen; insbesondere werden die Art der Daten, die Zweckbestimmung sowie die Dauer der geplanten Verarbei-tung, das Herkunfts- und Endbestimmungsland, die in dem betreffenden Drittland geltenden allgemeinen oder sektoriellen Rechtsnormen sowie die dort geltenden Standesregeln und Sicherheitsmaßnahmen berücksichtigt.“

Dieser Maßstab ist so unbestimmt und, durch eine Fülle von Ausnahmetatbe-ständen wie sie in Art. 26 vorgesehen sind, so löchrig, daß diese Regelung nicht geeignet zu sein scheint, das Problem der Datenoasen effektiv zu lösen.[39]

III. Datenschutz beim Schengen Information System (SIS) und bei Europol

1. Schengen Information System (SIS)

Aufgrund einer Initiative von Frankreich und der Bundesrepublik Deutschland wurden 1984 bilaterale Vereinbarungen zur Lockerung der Grenzkontrollen zwischen diesen beiden Staaten vereinbart. Daraufhin nahmen die Benelux-Staaten, die selbst schon seit den 60er Jahren inner-halb der Benelux-Grenzen auf Grenzkontrollen verzichtet haben, diese Initiative auf um das Deutsch-Fränzösische Abkommen auf die Benelux-Staaten zu erweitern.[40]

So kam es, daß im Jahre 1985 das Schengener Abkommen[41] zunächst zwischen Frankreich, Deutschland und den Benelux-Staaten beschlossen wurde. Im Zusammenhang mit der Abschaffung der Grenzkontrollen innerhalb der Schengen-Staaten wurde die Frage nach ihren Auswirkun-gen auf die grenzüberschreitende Kriminalität im Allgemeinen und der organisierten Kriminalität im Besonderen heftig diskutiert.[42] Die allgemein und ständig von allen Seiten gebetsmühlenhaft wiederholte Theorie ist, daß der Wegfall der Grenzkontrollen innerhalb der EG zu einer stark erhöhten grenzüberschreitende Kriminalität führe, welche durch eine Ver-stärkung der Kontrolle der Außengrenzen „auszugleichen“ sei.[43] Ob die Annahme, daß durch den Wegfall der Grenzkontrollen innerhalb der EG eine erhöhte (organisierte) Kriminalität einhergeht, richtig ist, erscheint zumindest zweifel-haft.[44] Jedenfalls gibt es hierzu keine gesicherten Kenntnisse. Vielmehr ist festgestellt worden, daß dem nicht so ist.[45] Dennoch war und ist diese Meinung verbreitet.

Kern des Schengener Abkommens ist, daß die Grenzkontrol-len zwischen diesen Staaten wegfallen sollen. Als Ausgleich für den „Sicherheitsverlust“ wurde ein ganzes Paket zur Verstärkung der polizei-liche Kooperation zwischen den Schengen-Staaten vereinbart.

Doch es dauerte bis 1990 um ein Übereinkommen zur Durchführung des Schengener Abkommens[46] (sog. Schengen Konvention oder Schengen II) mit detaillierten Regelungen zu beschließen, das zudem erst im Laufe des Jahres 1993 von allen Unterzeichnerstaaten ratifiziert wurde.

In diesem Abkommen wurde die polizeiliche Zusammenarbeit zwischen den Schengen-Mitgliedstaaten detailliert vereinbart. Hierzu gehört insbe-sondere die Schaffung des Schengen Information Systems (SIS).[47]

Kern-stück des SIS ist die Vernetzung der polizeilichen Datenbanken der Schengen-Mitgliedstaaten. Hierfür wurde ein Zentralrechner in Straßburg und in allen Schengen-Staaten nationale Zentralrechner mit identischem Datensatz installiert, der nach erheblichen technischen Anfangsproblemen seit einiger Zeit in Betrieb ist. Alle Polizeistationen der Schengen-Mitgliedstaaten haben Zugriff auf die Daten des Zentralrechners.

Aber nicht nur die Polizei- und Grenzstationen haben Zugriff auf den Zentralrechner, sondern auch Nachrichtendienste, denn nicht in allen Schengen-Staaten, beispielsweise in Frankreich, existiert die strenge Trennung zwischen der Polizei und den Nachrichtendiensten, wie sie in der Bundesrepublik Deutschland vorgesehen ist.[48]

Bei dem Schengener Abkommen handelt es sich, um ein Abkommen, welches auf den ersten Blick rechtlich mit der Europäischen Gemeinschaft wenig zu tun haben scheint.

Trotzdem besteht ein enger räumlicher und rechtlicher Zusammenhang mit der EG. Zum einen sollte Schengen als Modell für die geplante EG-weite Abschaffung der Grenzkontrollen dienen, um entsprechende Erfahrungen zu sammeln. Außerdem sind mittlerweile fast alle EG-Mitgliedstaaten der Schengen Konvention beigetreten oder beabsichtigen dies zu tun. Zum anderen enthält die Schengen Konvention zwei Artikel, welche explizit auf das Gemeinschaftsrecht verweisen (Art. 134 und 142 der Schengen Kon-vention).[49] Gem. Art. 134 findet die Schengen Konvention nur soweit Anwendung als sie nicht gegen Gemeinschaftsrecht verstößt. Sollten die Mitgliedstaaten der EG Regelungen zur Verwirklichung eines Raumes ohne Binnengrenzen beschließen, so sollen die Vertragsparteien der Schengen Konvention die Bestimmung daraufhin überprüfen, ob sie er-setzt oder geändert werden

müssen (Art. 142). Damit wird deutlich, wie eng die Schengen Konvention mit dem Gemeinschaftsrecht verzahnt ist.

Von besonderem Interesse ist nun die Frage, welche Daten und von wem im SIS gespeichert und verarbeitet werden sollen. Hierfür enthält Art. 94 eine abschlie-ßende Aufzählung. Neben Standardangaben wie Name, Geburtstag, -ort, Staatsangehörigkeit ist besonders Art. 94 III b hervorzuheben, wonach „besondere unveränderliche physische Merkmale“ gespeichert werden sollen. Fraglich ist, was darunter zu verstehen ist. Da es sich um unver-änderliche physische Merkmale handelt, kommen nur Daten über Rasse, Hautfarbe, digitalisierte Fingerabdrücke und digitalisiert DNA-Profile in Betracht.[50]

In den Art. 95 - 99 ist bestimmt von welchen Personengruppen personen-bezogene Daten im SIS gespeichert werden sollen. Unter anderem sollen Daten von Personen gespeichert werden, für die ein Haftbefehl ausgestellt ist, abgelehnte Asylbewerber und Personen, von denen die Gefahr der Begehung einer zukünftigen Straftat, ausgeht.

Besondere Hervorhebung gebührt in diesem Zusammenhang Art. 99 II b, wonach die Datenspeicherung zur „verdeckten Registrierung“ dieser Per-sonen zum Zwecke der Strafverfolgung und zur Abwehr von Gefahren für die öffentliche Sicherheit zulässig ist, wenn „die Gesamtbewertung des Betroffenen, insbesondere aufgrund der bisher von ihm begangenen Straftaten, erwarten läßt, daß er auch künftig außergewöhnlich schwere Straftaten begehen wird.“

Dieser Tatbestand ist dermaßen weit und offen, daß er ein Mindestmaß an Bestimmtheit vermissen läßt.[51] Hier wird der extreme präventive Charak-ter der Schengen Konvention deutlich.

Eine weitere Frage ist die nach den Rechten der Betroffenen. In Art. 109 ist das Recht vorgesehen, daß der Betroffene Auskunft über die zu seiner Person gespeicherten Daten hat. Wobei dieses Recht sich nach dem natio-nalen Recht der Vertragspartei, in deren Hoheitsgebiet das Auskunftsrecht beansprucht wird richtet. In Art. 110 ist das Recht der Berichtigung von unrichtigen Daten oder die Löschung von unrechtmäßig gespeicherten Daten enthalten. Schließlich ist in Art. 111 ein Klagerecht vorgesehen, vor dem nach nationalem Recht zuständigen Gericht.[52]

2. Europol

Im Gegensatz zum SIS basiert Europol rechtlich auf dem Maastricht Ver-trag. In Titel VI, Art. K.1 Nr. 9 - also im Bereich der sog. „dritten Säule der Europäischen Union“[53] - ist die Schaffung von Europol vorgesehen. In diesem Artikel sind auch die Angelegenheiten, welche von „gemeinsamen Interesse“ sind, aufgezählt. Hierzu gehört insbesondere die Asylpolitik (Art. K.1 Nr. 1), die Einwanderungspolitik (Art. K.1 Nr. 3), die Bekämp-fung der Drogenabhängigkeit (Art. K.1 Nr. 4), die Bekämpfung von Betrügereien im internationalen Maßstab (Art. K.1 Nr. 5), die Zusammen-arbeit in Zivil- und Strafsachen (Art. K.1 Nr. 6+7) und von großer Bedeu-tung die polizeiliche Zusammenarbeit zur Verhütung und Bekämpfung des illegalen Drogenhandels und sonstiger schwerwiegender Formen der internationalen Kriminalität (Art. K.1 Nr. 9).

Bemerkenswert hierbei ist, daß es sich um eine rein inter-governmentale Zusammenarbeit handelt und somit aus dem System der EG herausfällt. Daher mußte für Europol eine eigene rechtliche Grundlage geschaffen werden. Doch die EU-Mitgliedstaaten konnten sich lange Zeit nicht auf eine Europol-Konvention, welche die rechtliche Grundlage bilden sollte, einigen. So wurde die Errichtung von Europol in zwei Stufen vereinbart. Danach wurde als Vorläufer für die Europol die European Drugs Unit (EDU) geschaffen, die nur im Bereich der Drogenkriminalität arbeiten soll. Die EDU beruht auf eine Ministervereinbarung der Innen- und Justiz-minister vom 2.6.1993. Durch eine ergänzende Ministervereinbarung am 10.3.1995 wurde der Aufgabenbereich von Europol auf den illegalen Nuklearhandel, die Schleußerkriminalität und die Verschiebung von Kfz erweitert. Seit Januar 1994 arbeitet die EDU mit Sitz in Den Haag.

In der Ratstagung in Cannes im Juni 1995 wurde endlich die Europol-Konvention beschlossen[54], obwohl zwischen den Mitgliedstaaten immer noch Meinungsver- schiedenheiten hinsichtlich der

gerichtlichen Kontrolle durch den Europäischen Gerichts- hof bestehen. Aus diesem Grund hat noch kein Mitgliedstaat mit der Ratifizierung der Europol-Konvention begonnen.[55]

Um nun die Frage des Datenschutzes beurteilen zu können, scheint es geboten kurz auf die Arbeitsweise von Europol einzugehen.

Jeder Mitgliedstaat entsendet Verbindungsbeamte zu Europol. Diese Verbindungsbeamte haben Zugriff auf die jeweils nationalen Datenbanken und tauschen ihre Daten mit den Verbindungsbeamten der anderen Mit-gliedstaaten aus. In Art. 2 II sind die oben bereits erwähnten Aufgaben-gebiete genannt, wobei in zwei Jahren die präventive und repressive Terrorismusbekämpfung dazu kommen soll.[56]

Konkret soll Europol gem. Art. 3 I Daten sammeln, zusammenstellen und analysieren. Dabei wird Europol jeweils mit einer nationalen Stelle kom-munizieren, was im Falle der BRD das BKA sein wird. Das BKA soll die Daten an Europol liefern, wobei keine nachrichtendienstlichen Daten weitergeleitet werden sollen (Art. 4 V). Doch Europol wird nicht nur die Daten aus den Mitgliedstaaten sammeln, sondern hat auch die Be-fugnis eigene Daten zu sammeln und in die Europol-Datenbank einzuge-ben (Art. 8 III S. 3). Schließlich darf Europol Daten an „Drittstellen“ lie-fern, wenn „ein angemessener Datenschutz gewährleistet ist“ (Art. 18 I),[57] somit kann Europol an das SIS Daten liefern.

Darüber hinaus soll Europol - wie das SIS - Präventivspeicherung im großen Stil betreiben dürfen. Gem. Art. 8 I Nr. 2 soll die Datenverarbei-tung über Personen erlaubt sein „bei denen bestimmte Tatsachen die An-nahme rechtfertigen, daß sie Straftaten begehen werden“, ohne das eine konkrete Gefahr oder eine einschlägige Vortat vorzuliegen braucht.[58]

Der Datenschutz soll dem der EuDSK entsprechen (Art. 14), womit das gleich niedrige Datenschutzniveau wie beim SIS erreicht wird. Die Daten-schutzkontrolle ist wegen der besondere Arbeitsweise mittels der Verbin-dungsbeamte zweigeteilt. Danach wird die Eingabe und der Abruf der nationalen Stellen durch die nationalen Datenschutzbehörden kontrolliert. Die originäre Arbeit der Europol wird von einer „Gemeinsamen Kon-trollinstanz“ überwacht.

Auch ein Auskunftsrecht ist vorgesehen (Art. 19), wobei die Auskunft aus Sicherheitsgründen ohne Begründung verweigert werden kann.

Schließlich bekommt das Europäische Parlament einen jährlichen Tätig-keitsbericht von Europol.[59]

3. Bewertung

a) SIS
Hinsichtlich des SIS ist festzustellen, daß das Datenschutzniveau nicht höher ist, als das der EuDSK, so auch ausdrücklich Art. 126 der Schen-gen Konvention.[60] Dies ist sehr bedauerlich, da beim SIS hochsen-sible Daten gespeichert und verarbeitet werden und das von der EuDSK garantierte Schutzniveau hierfür völlig unzureichend ist. Hinzu kommt die Vernetzung der Datenbanken zwischen den Schengen-Staaten, die es für den Betroffenen praktisch unmöglich macht festzustellen, wer wo welche Daten von ihm gespeichert oder verarbeitet hat. Ein besonders anschau-liches Beispiel hierfür bietet Art. 46 der Schengen Konvention.

Gem. Art. 46 I kann jede Vertragspartei „nach Maßgabe ihres nationalen Rechts ohne Ersuchen im Einzelfall der jeweils betroffenen Vertragspartei Informationen mitteilen, die für den Empfänger zur Unterstützung bei der Bekämpfung zukünftiger Straftaten, zur Verhütung einer Straftat oder zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung von Bedeutung sein können.“

Hier ist die Tür für eine intensive und unkontrollierbare grenzüberschrei-tende Präventivspeicherung weit offen,[61] was aus rechtsstaatlichen Gründen inakzeptabel ist.[62]

Darüber hinaus haben es die Schengen-Staaten unterlassen die Vorausset-zungen für die Erhebung, Verarbeitung und Übermittlung in das SIS an-zugleichen, so daß hier erhebliche Unterschiede bestehen. Gleiches gilt für die Rechte der Betroffenen, welche jeweils unterschiedlich ausgestaltet sind.

Festzustellen bleibt daher, daß von einem einheitlichen Rechtsraum inner-halb der Schengen Konvention keine Rede sein kann.[63] Das Niveau des Datenschutzes wird beim SIS somit vom schwächsten Glied determi-niert.[64] Weiterhin läßt sich feststellen, daß durch die Einführung des SIS in bezug auf die europäische polizeiliche Datenverarbeitung und Koopera-tion eine ganz neue quantitative wie qualitative Dimension erreicht wurde.[65]

Ein entsprechend hohes Datenschutzniveau ist durch die Schengen Kon-vention jedoch nicht gewährleistet.[66] Schließlich fehlt eine ausreichende rechtliche oder parlamentarische Kontrolle.[67]

b) Europol

Wie beim SIS sind strukturelle Ähnlichkeiten, was die Befugnisse und den Datenschutz betrifft, vorhanden. Auch bei Europol wird die EuDSK das höchste Schutzniveau darstellen. Auch in diesem Fall ist dies ein völlig unzureichender Datenschutz, das wird vor allem deutlich, wenn man bedenkt, daß Europol ebenfalls im erheblichen Ausmaß Daten aus rein präventiven Gründen speichern darf.[68]

Darüber hinaus ist festzustellen, daß die Datenweitergabe von Europol an SIS gegen die Mindestanforderungen wie etwa die Erhebungsbeschränkung, die Zweckbestimmung und der Verwendungsbeschränkung verstößt. Dies ist eine bedenkliche datenschutzrechtliche Entwicklung ist, aber aus der Sicht einer noch effi-zienteren polizeilichen Kooperation nur konsequent.

Weiterhin stellt sich die Frage, ob langfristig der Austausch von Daten nur über die Verbindungsbeamte erfolgen wird, oder ob es nicht, um die Effi-zienz von Europol zu steigern, dazu kommen wird, daß alle Verbindungs-beamte Zugriff auf alle nationalen Datenbanken haben werden.[69]

Schließlich darf auch im Falle von Europol der Hinweis auf die völlig un-zureichende parlamentarische und rechtliche Kontrolle nicht fehlen.

IV. Ergebnis und Ausblick

Zunächst läßt sich als Ergebnis der Untersuchung feststellen, daß sich auf verschiedenen Ebenen im Rahmen unterschiedlichen Institutionen eine immer engere Zusammenarbeit im polizeilichen Bereich in Europa, sei es innerhalb der EU oder innerhalb der Schengen Konvention, entwickelt. Kernstück dabei ist die Intensivierung der computergestützen Datenspei-cherung, -austausch, -verarbeitung und -analyse[70].

Die Frage nach dem Datenschutz in Europa ist daher differenziert zu beur-teilen.

Die Datenschutzrichtlinie bietet, wie ausgeführt wurde, ein begrüßenswert hohes - teilweise höheres - Schutzniveau als das BDSG. Dennoch bleiben einige Probleme ungelöst, insbesondere bezüglich der „Datenoasen“. Trotzdem darf man realistischer- weise davon ausgehen, daß ein höheres Schutzniveau nicht möglich war, angesichts der Tatsache, daß einige EU-Mitgliedstaaten überhaupt kein Datenschutzgesetz haben oder eines mit sehr viel niedrigerem Schutzniveau. Hervorzuheben ist hierbei die Gleich- behandlung von öffentlich-rechtlichem und privatrechtlichem Bereich. Da schon seit einiger Zeit die technische Entwicklung zeigt, daß die datenschutzrechtlich relevanten personenbezogenen Datenerhebungen und -verarbeitungen zunehmend im privatrecht- lichen Bereich stattfinden.[71] Dies wird sich durch die andauernde Ausbreitung der on-line Dienste jeg-licher Art, sei es Internet oder andere kommerzielle Dienste, noch ver-stärken.

Dagegen hat der Datenschutz im weitaus sensibleren Bereich der polizei-lichen Kooperation einen sehr viel schlechteren Stand. Zur Erinnerung, die Datenschutz- richtlinie gilt nicht für Teil VI des EUV (Art. 3 II) - also nicht für Europol.

Aber auch in diesem Bereich ist zwischen SIS und Europol zu differenzie-ren. Beim SIS ist zumindest ein Mindestmaß an Datenschutz gewährlei-stet. Auch die Rechte der Betroffenen hinsichtlich Auskunft, Löschung und Berichtigung werden anerkannt.

Doch bei Europol ist dies alles nicht der Fall. So daß hier praktisch kein Datenschutz vorhanden ist. Dies ist um so bedauerlicher, da auch im Fall von Europol mit hoch sensiblen personenbezogenen Daten für ein breites Spektrum von Aufgaben und Befugnissen hantiert wird.

Darüber hinaus ist die rechtlich und gerichtliche Kontrolle bei Europol so kompliziert und mit hohen Hürden geregelt, daß sie faktisch nicht exi-stiert, wie Art. 19 und Art. 20 des Konventionsentwurfes zeigen.[72]

Dies wird noch dadurch verstärkt, daß SIS und Europol nur im Rahmen inter-governmentaler Zusammenarbeit bestehen und damit die rechtliche oder parlamen- tarische Kontrolle gänzlich fehlt.

Es entwickelt sich somit kein kohärentes Datenschutzsystem in Europa. Vielmehr ist ein zersplittertes - mit unterschiedlichem Schutzniveau aus-gestaltetest - nebeneinander laufendes Sammelsurium von Datenschutzre-gelungen für die unterschiedlichen Regime im Entstehen.[73]

Insoweit kann man sich des Eindrucks nicht erwehren, daß mittels der inter-governmentalen Zusammenarbeit - unter dem Deckmantel der Effektivität - die nationalen strengeren Datenschutzregelungen unterminiert und ausgehebelt werden könnten bzw. sollen. Zumindest eröffnet die inter-governmentale Zusammenarbeit die Etablierung von Strukturen und Arbeitsweisen, welche auf nationaler Ebene aufgrund der parlamentarischen und gerichtlichen Kontrolle so nicht möglich wären.

Ein weiteres schwerwiegendes Problem ist die Stellung von Nicht-EU-Bürgern, Asylanten und Asylsuchenden. Hier zeigt sich die „Festung Europas“ in seiner menschenverachtensten Form.[74] In dieser Festung ist durch die enumerative Aufzählung dieser Personengruppen als Zielgruppe - inhärent - die völlig unberechtigte Diskriminierung von allen Nicht-EU-Bürgern eingebaut worden, nur um den übertrieben Ruf nach populistischen Maß-nahmen im Kampf gegen alle Formen der Kriminalität, ohne die Effektivi-tät dieser Maßnahmen oder die negativen Auswirkung zu überprüfen, zu folgen.

Weiterhin ist deutlich geworden, daß der Anwendungsbereich und die Befugnisse bei SIS und Europol so weit gefaßt worden sind, daß eigent-lich alles möglich ist.

Ein weiterer wichtiger Faktor ist die technische Entwicklung der Informa-tions- technologie. Wenn der rasante Fortschritt, Verdoppelung der Lei-stungsfähigkeit pro Jahr, weiter anhält, werden dem Datenaustausch, Ab-gleich etc. noch weit mehr Möglichkeiten offen stehen.

In diesem Zusammenhang muß auch die zunehmende Kooperation auf nationaler wie internationaler Ebene gesehen werden. Es werden immer mehr polizeiliche und nachrichtdienstliche Datenbanken eingerichtet. Dies immer unter dem Gesichtspunkt der zunehmenden präventiven Polizeiar-beit. Dabei ist zu beachten, daß auch die Leistungsfähigkeit der Daten-banken ständig zunimmt, so daß immer komplexere Daten ohne weiteres gespeichert und ausgetauscht werden können. Als Beispiel sei hier auf die Vorbereitungen für ein europäisches automatisiertes Erkennungsdienst-system (EURODAC) für Flüchtlinge in allen EG-Mitgliedstaaten, die be-reits begonnen haben, verwiesen. Hierbei sollen die Fingerabdrücke digi-talisiert werden, genauso wie dies schon lange durch das AFIS-System (Automated Fingerprint Identification System) des FBI[75] und seit Dezem-ber 1992 auch des BKA bereits geschieht, um sie europaweit Abrufen zu können.[76] Als nächste Stufe dürfte, wie bereits in den liberalen Nieder-landen(!) geschehen, die Errichtung einer digitalisierten DNA-Profil-Datenbank anstehen, welche dann auch europaweit genutzt werden könnte.[77] Damit wird eine nochmalige qualitative Steigerung der Daten und der Datenverarbeitungsmöglichkeiten erreicht.

Geht man weiter davon aus, daß die polizeiliche Zusammenarbeit innerhalb und außerhalb Europas stetig zunehmen wird, so ist eines absehbar: der Daten-schutz wird immer das Nachsehen haben.

Im Endeffekt sind es zwei Ziele, die im EGV und EUV festgeschrieben sind, welche den Datenschutz verdrängen. Zum einen die Errichtung des freien Datenverkehrs- binnenmarktes und zum anderen die Bestrebung die (organisierte) Kriminalität mit allen Mitteln zu bekämpfen.

An dieser Stelle muß nachdrücklich betont werden, daß die Problematik der grenzüberschreitenden (organisierten) Kriminalität und der Asylpro-blematik nicht verharmlost werden sollen. Auch ist der

Ansatz, daß diese Probleme nur durch europaweite Maßnahmen zu lösen sind, richtig. Daß dafür auch die modernste Technik genutzt wird, ist selbstverständlich. Doch darf im Eifer des Gefechts nicht vergessen werden, daß die Mit-gliedstaaten von Schengen und EU, auch die Grundrechte aller Bürger zu wahren haben. Dies wird im übrigen schon durch Art. 1 I der EMRK zum Ausdruck gebracht. Hierbei kommt „dem Datenschutz eine Basisfunktion zu.“[78]

Literaturverzeichnis

Bäumler, H. Datenschutz für Ausländer, Datenschutz und Datensicherheit 1994, S. 540 - 542.

Bieber, R. Die Abkommen von Schengen über den Abbau der Grenzkontrollen, NJW 1994, 294 - 297.

Boeles, P. Data Exchange, Privacy and Legal Protection, in: Free Movement of Persons in Europe, Asser Instituut Colloquium on European Law, Session XXI, 1991, S. 52 - 74, edited by Schermers, Flinterman, Kellerman, Haersolte, van de Meent, Dordrecht, Boston, London 1993.

Busch, H. Europa - „ein Mekka der Kriminalität“?, Kritische Justiz 1990, S. 1 - 13.

D’Oliveira, H.U. Expanding external and shrinking internal borders:Europe’s defence mechanisms in the areas of free movement, immigration and asylum, in: Legal Issues of the Maastricht Treaty, S. 267 - 278, edited by O’Keeffe, Twomey, London, New York, Chichester, Brisbane, Toronto, Singapore 1994.

den Boer, M. Police Co-operation in the EU: Tiger in a Trojan horse?, Common Market Law Review 1995, S. 555 - 578.

Europe and the art of international police co-operation: free fall or measured scenario? in: Legal Issues of the Maastricht Treaty, S. 279 - 291, edited by O’Keeffe, Twomey, London, New York, Chichester, Brisbane, Toronto, Singapore 1994.

Ellger, R. Konvergenz oder Konflikt bei der Harmonisierung des Datenschutzes in Europa?, Computer und Recht 1994, S. 558 - 569.

Der Datenschutz im grenzüberschreitenden Datenverkehr: eine rechtsvergleichende und kollisionsrechtliche Untersuchung, 1. Aufl., Baden-Baden 1990.

Fijnaut, C.J.C.F. The Schengen Treaties and European Police Co-operation, European Journal of Crime, Criminal Law and Criminal Justice 1993, S. 37 - 56.

The „Communitization“ of Police Co-operation in Western Europe, in: Free Movement of Persons in Europe, Asser Instituut Colloquium on European Law, Session XXI, 1991, S. 75 - 92, edited by Schermers, Flinterman, Kellerman, Haersolte, van de Meent, Dordrecht, Boston, London 1993.

Hahn, U. Datenschutzrecht und grenzüberschreitender Datenverkehr: Regelungsbedarf, Rechtsvergleich und Rechtsfortbildung, Frankfurt/M., Berlin, Bern, New York, Paris, Wien, 1994.

Hassemer, W. Datenschutz für Ausländer?, Datenschutz und Datensicherung, 1994, S. 538 - 539.

Zeit zum Umdenken, Datenschutz und Datensicherung, 1995, S. 448 - 449.

Kampen, P./ Nijboer, H. DNA fingerprinting in the Dutch Code of Criminal Procedure, Expert Evidence 1994, S. 70 - 74.

Korff, D. Der EG-Richtlinienentwurf über Datenschutz und„anwendbares Recht“, Recht der Datenverarbeitung 1994, S. 209 - 217.

Kühne, H.H. Kriminalitätsbekämpfung durch innereuropäische Grenzkontrollen? Auswirkungen der Schengener Abkommen auf die innere Sicherheit, Berlin 1991.

Lavranos, N. DNA-Profiling and Information Technology: A new weapon for Crime Detection and Prevention?, European Journal of Crime, Criminal Law and Criminal Justice 1994, S. 359 - 378.

Mähring, M. Das Recht auf informationelle Selbstbestimmung im europäischen Gemeinschaftsrecht, Europarecht 1991, S. 369 - 374.

Nutger, A.C.M. Transborder Flow of Personal Data within the EC, Deventer, Boston, 1990.

O'Keeffe, D. The Schengen Convention: A suitable Model for European Integration?, Yearbook of European Law, Vol. 11 (1991), Oxford 1992.

Oppermann, Th. Europarecht, München 1991.

Pernice, I, Gemeinschaftsverfassung und Grundrechtsschutz Grundlagen, Bestand und Perspektiven, NJW 1990, S. 2409 - 2420.

Riegel, R. Zum Verhältnis von Recht und Wirklichkeit am Beispiel des Datenschutzrechts in der Europäischen Gemeinschaft, DÖV 1991, S. 311 - 319.

Grenzen informationeller Zusammenarbeit zwischenPolizei und Verfassungsschutz, DVBl 1988, S. 121 - 129.

Schattenberg, B. The Schengen Information System: Privacy and Legal Protection, in: Free Movement of Persons in Europe, Asser Instituut Colloquium on European Law, Session XXI, 1991, S. 43 - 51, edited by Schermers, Flinterman, Kellerman, Haersolte, van de Meent, Dordrecht, Boston, London 1993.

Schutte, J. Schengen: It's Meaning for the free movement of persons in Europe, Common Market Law Review 1991, S. 549 - 570.

Simitis, S. Das scheinbar Private ist längst öffentlich, Frankfurter Rundschau v. 19.6.1995, S. 9.

Simitis,S./ Daten ohne Grenzen, Bürger ohne Schutz? –
Fuckner, G. Datenschutz und Innere Sicherheit in Europa, in: Innere Sicherheit im europäischen Binnenmarkt, S. 337 - 355, Veröffentlichung der Bertelsmann Stiftung / Rupprecht/Hellenthal, Gütersloh 1992.

Streinz, R. Europarecht, 2. Aufl., Heidelberg 1995.

Tinnefeld, M.-T. Datenschutz - Baustein im europäischen Integrationsprozeß, Datenschutz und Datensicherung 1993, S. 555 - 560.

Verhey, L.F.M. Privacy aspects of the Convention Applying theSchengen Agreement, in: Schengen, Internationalisation of central chapters of the law on aliens, refugees, privacy, security and the police, S. 110 - 134, edited by Meijers, Bolten, Cruz, Steenbergen, Hoogenboom, Swart, Verhey, Boeles, Deventer, Boston 1991.

Weichert, T. Europa - Gemeinschaft der Inneren Sicherheit, Datenschutz-Nachrichten 1993, S. 12 - 16.

Datenschutz für Asylsuchende, Datenschutz-Nachrichten 1994, S. 8 - 10.

Europol-Konvention und Datenschutz, Datenschutz und Datensicherheit 1995, S. 450 - 458.

Wind, I./ Entwurf für eine EG-Richtlinie zum Datenschutz,

Siegert, M. Computer und Recht 1993, S. 46 - 55.

Datenschutzrichtlinie der EG - mögliche Auswirkungen auf das BDSG, Recht der Datenverarbeitung 1992, S. 118 - 121.

Wurst, M. Europa 1992 - Auf dem Weg zu einem einheitlichen Datenschutzrecht in der Europäischen Gemeinschaft, JuS 1991, S. 448 - 453.

---

[1] Näher hierzu: Ellger, S. 87 f.

[2] Ausführlich zur historischen Entwicklung des Datenschutzes auf internationaler Ebene siehe: Hahn, S. 47 ff.

[3] Hahn, S. 81 ff.; Wurst, JuS 1991, S. 448 f.

[4] Vgl.: Fijnaut, Eur. J. Crime.Cr.L.Cr.J. 1993, S. 37 f.; O'Keeffe, YEL 1991, S. 201.

[5] BVerfGE 65, S. 1 ff.

[6] Zur Frage in wie weit ein Grundrechtsschutz im Gemeinschaftsrecht dennoch besteht siehe: Pernice, NJW 1990, S. 2409 ff.

[7] NJW 1993, S. 3047 ff.

[8] Wörtlich heißt es dazu im Maastricht-Urteil:„Die in der Präambel des Grundgesetzes angelegte und in Art. 23 und 24 GG geregelte Offenheit für eine europäische Integra- tion hat zur Folge, daß grundrechtserhebliche Eingriffe auch von europäischen Organen ausgehen können und ein Grundrechtsschutz dementsprechend für das gesamte Geltungsgebiet dieser Maßnahme gewährleistet werden muß." (NJW 1993, S. 3049).

[9] Zu den rechtlichen Problemen die dabei entstehen können siehe: Streinz, Rn. 220 ff.

[10] Näher dazu siehe: Nutger, S. 284 ff.; Mähring, EuR 1991, S. 369 ff. m.w.N.; Oppermann, Rn. 85; Hahn, S. 64, Wurst, S. 451 ff.

[11] ABl. der EG Nr. L 281 vom 23.11.1995, S. 31 ff.

[12] Hierzu näher: Hahn, S. 47 ff.

[13] Vgl. Wurst, S. 450.

[14] Vgl. Hahn, S. 55 f.

[15] Ausführlich dazu: Hahn, S. 57 ff.

[16] Ellger, CR 9/1994, S. 560.

[17] Riegel, DÖV 1991, S. 316.

[18] Ausführlich zur Geschichte der Datenschutzrichtlinie siehe: Wurst, S. 448 f; Hahn S. 81 ff.

[19] ABl. Nr. C 277 vom 5.11.1990, S. 3.

[20] Zu den Änderungsvorschlägen des Europäischen Parlaments siehe: Wind/Siegert, RDV 1992, S. 118 ff.

[21] ABl. Nr. C 311 vom 27.11.1992, S. 30.

[22] Erwägungsgrund (3).

[23] Wind/Siegert, CR 1/1993, S. 47.

[24] Wind/Siegert, CR 1/1993, S. 48.

[25] Hassemer (DuD 1995, S. 448) formuliert dies sehr schön: „Die Informationstechno- logie von heute hat Zahn und Kralle perfekt laviert und tritt den Bürgern verführerisch entgegen: Zeit sparen, Trefferquoten erhöhen, Farbe in den Alltag bringen, neue Dimensionen erschließen. Kredit- und Gesundheitskarten, Telematik, interaktive Medien, Teleshopping, Datenautobahn, Biometrie - eine Informationstechnologie in bequemer und bunter Freizeitkleidung, welche mit der Uniform des Volkszählers scheinbar nichts mehr zu tun hat.“

[26] Ausführlich hierzu: Simitis, Frankfurter Rundschau v. 19.6.1995, S. 9.

[27] Wind/Siegert, CR 1/1993, S. 49.

[28] So auch Wind/Siegert, CR 1/1993, S. 55.

[29] Vgl. Riegel, S. 313.

[30] Riegel, S. 312.

[31] Näher zu diesem Punkt siehe: Riegel, S. 317.

[32] Ausführlich zu den verfassungsrechtlichen Implikationen siehe: Korff, RDV 1994, S. 209 ff.

[33] BVerfGE 65, S. 1 ff.

[34] NJW 1993, S. 3047 ff.

[35] Ausführlich zu diesem Punkt: Korff, S. 214.

[36] So Riegel, S. 313.

[37] Vgl. Nutger, S. 293 f.

[38] Ellger, S. 95 m.w.N.

[39] So auch Ellger, CR 9/1994, S. 564 f.

[40] Siehe hierzu: Fijnaut, Eur. J. Crime.Cr.L.Cr.J. 1993, S. 37 ff.; Kühne, S. 11.

[41] Abgedruckt bei Kühne, S. 84 ff.

[42] Vgl. Fijnaut, Asser Instituut, S. 86 ff.

[43] Ausführlich dazu: Kühne. S. 9 ff.

[44] Näher hierzu: Busch, KJ 1990, S. 1 ff.; Weichert, DANA 2/1993, S. 14.

[45] Busch (ebenda) macht jedenfalls deutlich, daß nach den Angaben des BGS die Grenzkontrollen nicht wesentlich zur Ermittlung und Überführung von grenzüber- schreitenden Straftaten bzw. Straftätern führen. So auch Bieber, NJW 1994 S. 295. Ganz anderer Auffassung ist hier Schattenberg, Erster Direktor des BKA, S. 43 ff.

[46] Abgedruckt bei Kühne, S. 89 ff.; BGBl 1993, S. 1013 ff.

[47] Näher hierzu: Fijnaut, Eur. J. Crime.Cr.L.Cr.J. 1993, S. 37 ff.

[48] Ob man im Fall der BRD tatsächlich noch von einer faktischen Trennung zwischen Geheimdiensten und Polizei bei der informationellen Zusammenarbeit sprechen kann, siehe hierzu kritisch: Riegel, DVBl 1988, S. 121 ff.

[49] Schutte, CML Rev. 1991, S. 566.

[50] Welche Möglichkeiten und Gefahren sich mit digitalisierten DNA-Profilen hinsicht- lich der präventiven polizeilichen Ermittlungen ergeben siehe ausführlich: Lavranos, Eur. J. Crime.Cr.L.Cr.J. 1994, S. 359 ff.

[51] O'Keeffe, S. 207; Boeles, Asser Instituut, S. 52.

[52] Ausführlich hierzu: O'Keeffe, S. 205 f.

[53] Zur besonderen Bedeutung der dritten Säule für die polizeiliche Zusammenarbeit siehe: den Boer, CML Rev. 1995, S. 555 ff.

[54] Ausführlich zum Entwurf der Europol Konvention siehe: den Boer, S. 568 ff.; Weichert, DuD 1995, S. 450 ff.; den Boer, S. 569 f.

[55] Siehe auch: European Voice v. 21.12.1995, S. 8.

[56] So Weichert, DuD 1995, S. 451.

[57] Vgl. den Boer, S. 570; Weichert, DuD 1995, S. 453.

[58] Vgl. Weichert, DuD 1995, S. 454.

[59] Vgl. Weichert, DuD 1995, S. 452.

[60] So auch Verhey, Schengen, S. 127; O'Keeffe, S. 206.

[61] Boeles, S. 53; Verhey, S. 126 f.

[62] O'Keeffe, S. 203.

[63] Vgl. Riegel, S. 314 f.

[64] Weichert, DANA 2/1993, S. 15.

[65] So auch Fijnaut, Eur. J. Crime.Cr.L.Cr.J. 1993, S. 37 f.; O'Keeffe, S. 201;

Simitis/Fuckner, S. 343; Busch, S. 10; Riegel, S. 314.

[66] Verhey, S. 133; Ganz anderer Auffassung ist dagegen Schattenberg, S. 43 ff.

[67] Bieber, S. 296; O'Keeffe, S. 212.

[68] Übereinstimmend Weichert, DuD 1995, S. 455.

[69] Auf das grundsätzliche Problem Tatsachen ohne rechtliche Grundlage zu schaffen, verweisen Simitis/Fuckner (S. 353):„Auch und gerade dann, wie etwa bei On-line-Anbindungen erklärt wurde, bestimmte Verarbeitungsmöglichkeiten lediglich erproben zu wollen, hat sich sehr schnell erwiesen, daß mit den 'Probeläufen' Verarbeitungs- strukturen entstanden, die allein schon der Kosten wegen nicht mehr rückgängig zu machen waren".

[70] So auch schon in: Lavranos, S. 375.

[71] Simitis, Frankfurter Rundschau, v. 19.6.1995, S. 9.

[72] Näher hierzu: Weicher, DuD 1995, S. 456.

[73] So auch den Boer, Legal Issues, S. 288; Bieber, S. 297.

[74] Ausführlich zu dieser Problematik: Boeles, S. 52 ff; D'Oliveira, S. 274 ff. Über die Nichtexistenz des Datenschutzes für Ausländer bereits innerhalb des deutschen Rechtssystems siehe: Bäumler, DuD 1994, 540 ff; Hassemer, DuD 1994, 538 f.

[75] Näher zu AFIS siehe: Lavranos, S. 377.

[76] Weichert, DANA 2/1993, S. 16, ders. DANA 5/1994, S. 9.

[77] Siehe hierzu: Kampen/Nijboer, Expert Evidence, S. 70 ff.

[78] Tinnefeld, DuD 1993, S. 556.